PU020267 DESCAF(Kathleen) (JP2000244547) ON 9180

(19) Patent Agency of Japan (JP)
(12) Official report on patent publication (A)
(11) Publication number: 2000-244547
(43) Date of publication of application: 08.09.2000
(51) Int.Cl. H04L 12/46 H04L 12/28 G09C 1/00
H04L 9/14 H04L 9/32 H04L 12/66
(21) Application number: 11-039196
(22) Date of filing: 17.02.1999
(71) Applicant: Nippon Telegr & Teleph Corp <NTT>
(72) Inventor: Kuno Yutaka, Hanazawa Tetsuo, Morikura Masahiro
(54) Title of the invention: Certification method
(57) Abstract:
Problem to be solved: To select a suitable encryption algorithm even when access to a home network is continued while moving between different types of networks.
Solution: On the basis of network information reported from an access network B, a mobile terminal judges the strength of a required cipher and selects the encryption algorithm. Afterwards, at the time of certification with the tunnel server of a home network A, the mobile terminal sends the class of the selected encryption algorithm and information capable of specifying this session while signing with the signature key thereof. The tunnel server verifies that signature and after the information capable of specifying this session reported from the mobile terminal is collated with information capable of specifying this session managed by the tunnel server, enciphered VPN

communication based on the selected encryption algorithm is started.

[Claims]

[Claim 1] In a certification method of a communications system which attests among tunnel servers and communicates by establishing an encryption tunnel between a moving terminal and a tunnel server by an access network and a transit network, including a tunnel server in a moving terminal, an access network, a transit network, a home network, a home network and a moving terminal, a moving terminal attests at the time of connection with an access network and intensity of a required code is judged based on network information notified from an access network at the time of attestation with an access network, classification of an encryption algorithm which chose an encryption algorithm and was chosen at the time of attestation with a tunnel server and information which can specify this session, signs and sends out with its own signature key and a tunnel server, based on a collated result of information which can specify this session that verified the mentioned above signature and was notified from a moving terminal and information which can specify this session that a tunnel server has managed, a certification method starting enciphered VPN communication by a selected encryption algorithm if the justification of a moving terminal is judged and justification is recognized.

[Claim 2] A certification method characterized by using access frequency from the outside of a moving terminal as information which can specify the mentioned above session in the certification method according to claim 1.
[Claim 3] A certification method using time information to which a session was carried out in the certification method according to claim 1 as information which can specify the mentioned above session.
[Claim 4] In a certification method of a communications system which attests among tunnel servers and communicates by establishing an encryption tunnel between a moving terminal and a tunnel server by an access network and a transit network, including a tunnel server in a moving terminal, an access network, a transit network, a home network, a home network and a moving terminal, a moving terminal attests at the time of connection with an access network and at the time of attestation with a tunnel server, network information notified from an access network at the time of attestation with information and an access network which can specify this session, signs and sends out with its own signature key and a tunnel server, based on a collated result of information which can specify this session that verified the mentioned above signature and was notified from a moving terminal and information which can specify this session that a tunnel server has managed, a certification method judging intensity of a required code, choosing an encryption algorithm and starting enciphered VPN communication by a selected encryption algorithm based on network information notified from a moving terminal if

the justification of a moving terminal is judged and justification is recognized.
[Claim 5] A certification method characterized by using access frequency from the outside of a moving terminal as information which can specify the mentioned above session in the certification method according to claim 4.
[Claim 6] A certification method using time information to which a session was carried out in the certification method according to claim 4 as information which can specify the mentioned above session.

[Detailed description of the invention]

[0001]
[Field of the invention] This invention relates to the certification method in the case of accessing a home network, performing seamless movement between different type networks.
[0002]
[Description of the prior art] In recent years, according to progress of mobile computing, the VPN (Virtual Private Network) art which accesses from the outside the network of the office in which a user is doing usual access is looking at development exceeding the firewall (firewall). The basis of VPN is establishment of the attestation and the encryption tunnel by the tunnel server in a firewall.
[0003] Drawing 3 is an explanatory view showing the example of an outline of the system by which a moving terminal performs access to the home network A from the exterior by the access networks (local area network) B, C, establishing VPN. The firewall is set up in this drawing only a certification packet with a tunnel server and the

packet passing through an encryption tunnel with a tunnel server pass.
[0004] Establishment of an encryption tunnel is performed by following procedure (1) – (3) (see drawing 4).
(1) A moving terminal and a tunnel server attest (2-a).
(2) Perform the negotiation of an encryption key (2-b).
(3) Establish an encryption tunnel (2-c).
[0005] As the time required according to decryption is generally decided by encryption trial frequency per unit time, there is a tendency which is easy to be decoded for a short time as a code with a quick encryption trial speed. Drawing 5 is a chart showing the relation between the characteristic (intensity and speed) of an encryption algorithm and a network. As shown on this table, the case of connection through a dedicated line and in connection through a local area network, high safety is not required, but also in order not to reduce the high access speed which the mentioned above dedicated line and the mentioned above local area network have, a high speed encryption algorithm is required. On the other hand, in connection through the Internet, as it is thought that the access speed of the transmission line (Internet) itself is low, a high speed encryption algorithm is not required, but high safety is required.
[0006] In a VPN system actually marketed now, (1) there is a system and the like which is using the simple code mainly being used in a local area network and (2) OCN which is using the powerful code used in commercial Internet services. As an example of the above (1), there is Logical Office (NTT R&D, a «logical office service»,

Vol.45 No.10 1996 Tanimoto). As an example of the above (2), there are DEC, NTT-AT by Altavista tunnel.
[0007]
[Problems to be solved by the invention] By the way, the communication configuration which performs communication continued while progress of standardization moved as a new usage pattern of remarkable wireless LAN in recent years ranging over between different type networks is becoming actual. As an example of this usage pattern, as shown on drawing 3, it is possible to change the access network through communication into the access network B from the access network C with movement of a moving terminal. In such a usage pattern, the encryption tunnel between a moving terminal and a home network will go by various communication paths.
[0008] Thus, in the conventional system (system by which only the single encryption algorithm is prepared), even if the prepared this encryption algorithm is a case where the processing speed demanded from the communication path which is carrying out the present course although it is safe more than needed is not being filled or although it was a high speed more than needed, even if it was a case where the safety demanded was not being filled, subject that the this prepared encryption algorithm had to be used occurred.
[0009] This invention was made under such a background and an object of an invention is to provide the certification method which can choose appropriately the encryption algorithm of required intensity and speed, even if it continues access to a home network, performing seamless movement between different type networks.

[0010]
[Means for solving the problem] The invention according to claim 1 includes a tunnel server in a moving terminal, an access network, a transit network, a home network, a home network and a moving terminal, in a certification method of a communications system which attests among tunnel servers and communicates by establishing an encryption tunnel between a moving terminal and a tunnel server by an access network and a transit network, a moving terminal attests at the time of connection with an access network and intensity of a required code is judged based on network information notified from an access network at the time of attestation with an access network, classification of an encryption algorithm which chose an encryption algorithm and was chosen at the time of attestation with a tunnel server and information which can specify this session, signs and sends out with its own signature key and a tunnel server, based on a collated result of information which can specify this session that verified the mentioned above signature and was notified from a moving terminal and information which can specify this session that a tunnel server has managed, if the justification of a moving terminal is judged and justification is recognized, enciphered VPN communication by a selected encryption algorithm will be started. The invention according to claim 2 uses access frequency from the outside of a moving terminal in the certification method according to claim 1 as information which can specify the mentioned above session. The invention according to claim 3 uses time information to which a session was carried out in the certification method according to claim 1 as information

which can specify the mentioned above session. The invention according to claim 4 includes a tunnel server in a moving terminal, an access network, a transit network, a home network, a home network and a moving terminal, in a certification method of a communications system which attests among tunnel servers and communicates by establishing an encryption tunnel between a moving terminal and a tunnel server by an access network and a transit network, a moving terminal attests at the time of connection with an access network and at the time of attestation with a tunnel server, network information notified from an access network at the time of attestation with information and an access network which can specify this session, signs and sends out with its own signature key and a tunnel server, based on a collated result of information which can specify this session that verified the mentioned above signature and was notified from a moving terminal and information which can specify this session that a tunnel server has managed, if the justification of a moving terminal is judged and justification is recognized, based on network information notified from a moving terminal, will judge intensity of a required code and an encryption algorithm will be chosen, enciphered VPN communication by a selected encryption algorithm is started. The invention according to claim 5 uses access frequency from the outside of a moving terminal in the certification method according to claim 4 as information which can specify the mentioned above session. The invention according to claim 6 uses time information to which a session was carried out in the certification method

according to claim 4 as information which can specify the mentioned above session.

[0011]

[Embodiment of the invention] §1. Outline

In this invention, a moving terminal and an access network perform mutual recognition at the time of connection with an access network, the information (information on a network address and hardware for operations) about this access network is acquired and it is characterized by choosing the encryption algorithm of required intensity and speed based on this information. While a moving terminal carries out movement which straddles between different type networks, it differs from conventional technology in that it can communicate by choosing the most suitable encryption algorithm at each time. It is possible according to this invention to judge the safety and speed according to the network which connects and to choose a suitable encryption algorithm, especially, in advanced mobile communication systems, such as wireless LAN, the effect which makes it possible to always continue accessing its office environment is acquired.

[0012] §2. The 1st embodiment

The 1st embodiment of this invention is described with reference to a drawing. Although this embodiment corresponds to claim 2, in the following explanation, replacing «frequency information» with «time information» by becoming the explanation corresponding to claim 3 and it becomes the explanation corresponding to claim 1 by replacing «frequency information» with «the information which can specify this session».

[0013] Drawing 1 is a sequence diagram showing an example of the certification method by the 1st embodiment of this invention. With this drawing, the case «where the moving terminal is communicating by establishing the home network A and a VPN encryption tunnel by the access network C» is considered like on drawing 3 as an initial state.
[0014] In this initial state, if a moving terminal moves like drawing 3, the access network used for communication will change from the access network C to the access network B. If it changes to the access network B, a moving terminal and the access network B will carry out mutual recognition of the public key certification.
[0015] A moving terminal chooses an encryption algorithm suitable for the access network B based on the network information in the certificate of the access network B at the time of mutual recognition with the access network B.
[0016] To the encryption algorithm selection message which shows the classification of the selected encryption algorithm, a moving terminal signs with a signature key peculiar to this moving terminal and sends out the signed encryption algorithm selection message to the termination node (tunnel server) of VPN of the home network A.
[0017] At this time, a moving terminal must prevent the mentioned above signature key (it asks by analyzing this signed encryption algorithm selection message) being diverted by the access network B. Next, a moving terminal signs to the encryption algorithm selection message which included the frequency information which shows the number of times which accessed the home network A from the exterior in the signature sentence (namely, encryption

algorithm selection message) and in which this frequency information was included. According to this, since the access network B cannot forge frequency information, it also becomes impossible to analyze and divert a signature key.

[0018] When the encryption algorithm selection message signed after frequency information was incorporated is received, the home network A, the frequency information (namely, the frequency information which the moving terminal has managed) from these receiving contents the following and the «moving terminal side frequency information» takes out and this moving terminal side frequency information is compared with the frequency information (the «home network side frequency information» is called next) which the home network A has managed about access to the home network A from the moving terminal.

[0019] If the moving terminal side frequency information and the home network side frequency information are not in agreement, the home network A will refuse connection with a moving terminal and will end processing. On the other hand, if the moving terminal side frequency information and the home network side frequency information are in agreement, the home network A will increase the home network side frequency information (shown number of times) by 1.

[0020] The home network A takes out an encryption algorithm selection message from the encryption algorithm selection message signed after frequency information was incorporated, a VPN encryption tunnel is established based on the encryption algorithm (namely, encryption algorithm

selected with the moving terminal) of the classification which this encryption algorithm selection message shows. Finally, a moving terminal increases the moving terminal side frequency information (shown number of times) by 1. Above, processing is ended.

[0021] According to the mentioned above certification method, even if it continues access to a home network, performing seamless movement between different type networks, the encryption algorithm of required intensity and speed can be chosen appropriately.

[0022] §3. The 2nd embodiment

The 2nd embodiment of this invention is described with reference to a drawing. Although this embodiment corresponds to claim 5, in the following explanation, replacing «frequency information» with «time information» by becoming the explanation corresponding to claim 6 and replacing «frequency information» with «the information which can specify this session», it becomes the explanation corresponding to claim 4.

[0023] Drawing 2 is a sequence diagram showing an example of the certification method by the 2nd embodiment of this invention. The case «the moving terminal is communicating by establishing the home network A and a VPN encryption tunnel by the access network C» like drawing 3 as an initial state with this drawing is considered too.

[0024] In this initial state, if a moving terminal moves like on drawing 3, the access network used for communication will change from the access network C to the access network B.

If it changes to the access network B, a moving terminal and the access network B will carry out mutual recognition of the public key certification.

[0025] At the time of mutual recognition with the access network B, to the network information in the certificate of the access network B, a moving terminal signs with a signature key peculiar to this moving terminal and sends out the signed network information to the termination node (tunnel server) of VPN of the home network A.

[0026] At this time, a moving terminal must prevent the mentioned above (it asks by analyzing this signed network information) signature key being diverted by the access network B. Next, a moving terminal signs to the network information which included the frequency information which shows the number of times which accessed the home network A from the exterior in the signature sentence (namely, the mentioned above network information) and in which this frequency information was included. According to this, as the access network B cannot forge frequency information, it becomes impossible to analyze and divert a signature key too.

[0027] When the network information signed after frequency information was incorporated is received, the home network A, frequency information (namely, the moving terminal side frequency information) is taken out from these receiving contents and this moving terminal side frequency information is compared with the frequency information (namely, the home network side frequency information) which the home network A has managed about access to the home network A from the moving terminal.

[0028] If the moving terminal side frequency information and the home network side frequency information are not in agreement, the home network A will refuse connection with a moving terminal and will end processing. On the other hand, if the moving terminal side frequency information and the home network side frequency information are in agreement, the home network A will increase the home network side frequency information (shown number of times) by 1.

[0029] The home network A takes out network information from the network information signed after frequency information was incorporated and chooses an encryption algorithm suitable for the access network B based on this network information. The home network A establishes a VPN encryption tunnel based on this chosen encryption algorithm. Finally, a moving terminal increases the moving terminal side frequency information (shown number of times) by 1. Above, processing is ended.

[0030] According to the mentioned above certification method, even if it continues access to a home network, performing seamless movement between different type networks, the encryption algorithm of required intensity and speed can be chosen appropriately.

[0031] §4. Capture

Although, the embodiment of this invention is explained in full details with reference to drawings, concrete composition is not restricted to this embodiment and even if there are change and the like of a design of the range which does not deviate from the gist of this invention, it is included in this invention.

[0032]
[Effect of the invention] As explained above, as an encryption algorithm can be chosen based on the network information about an access network according to this invention, the encryption algorithm provided with required safety and processing speed can be chosen appropriately. In particular, in mobile computing using wireless LAN, it can move now seamlessly by this invention between different type networks. As the necessity of making a user purchasing 2 of systems (the system for local area networks and the system for commercial internets) which were explained by the paragraph of «prior art» is lost, as a system vendor, economy of scale is enjoyable.

[Brief description of the drawings]

[Drawing 1] is a sequence diagram showing an example of the certification method by the 1st embodiment of this invention.
[Drawing 2] is a sequence diagram showing an example of the certification method by the 2nd embodiment of this invention.
[Drawing 3] is an explanatory view showing the example of an outline of the system which communicates by establishing VPN.
[Drawing 4] is a sequence diagram showing an example of a procedure which establishes an encryption tunnel.
[Drawing 5] is a chart showing the relation between the characteristic and a network (intensity and speed) of an encryption algorithm.

```
ERROR: undefinedresource
OFFENDING COMMAND: findresource

STACK:

/DefaultColorRendering
/ColorRendering
/DefaultColorRendering
```